526 Rec'd PCT/PTO 08 JUN 2000

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **RCA88783**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/581064**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US98/26069	**09 DECEMBER 1998**	**10 DECEMBER 1997**

TITLE OF INVENTION

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

APPLICANT(S) FOR DO/EO/US

AHMET MURSIT ESKICIOGLU, MEHMET KEMAL OZKAN AND BILLY WESLEY BEYERS, JR.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

RETURN RECEIPT POSTCARD

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR) 09/581064	INTERNATIONAL APPLICATION NO. PCT/US98/26069	416 Rec'd PCT/PTO 08 JUN 2000 ATTORNEY'S DOCKET NUMBER RCA88783

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$970.00**
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	**$840.00**
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$690.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$670.00**
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	**$96.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$840.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	7 - 20 =	0	x $18.00	**$0.00**	
Independent claims	2 - 3 =	0	x $78.00	**$0.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS			=	**$840.00**	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	**$0.00**	
SUBTOTAL			=	**$840.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE			=	**$840.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	**$0.00**	
TOTAL FEES ENCLOSED			=	**$840.00**	
				Amount to be: refunded	$
				charged	$

☐ A check in the amount of to cover the above fees is enclosed.

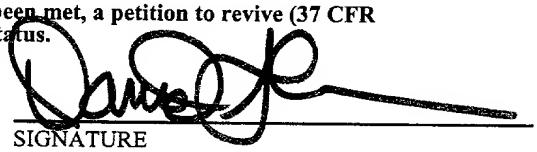
☒ Please charge my Deposit Account No. **07-0832** in the amount of 840.00 to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **07-0832** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

JOSEPH S. TRIPOLI - PATENT OPERATIONS
THOMSON MULTIMEDIA LICENSING, INC.
PO BOX 5312 - 2 INDEPENDENCE WAY
PRINCETON, NJ 08543-5312



SIGNATURE

DAVID T. SHONEMAN
NAME

39,371
REGISTRATION NUMBER

6/8/00
DATE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Ahmet Mursit Eskicioglu et al.

Int'l. Appl. No. : PCT/US98/26029

Int'l. Filing No : 09 December 1998 (09.12.98)

For : CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

PRELIMINARY AMENDMENT

Honorable Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In the US national phase application of PCT/US98/26029 filed herewith, please enter the following amendments:

Please amend the claims as follows:

In the Claims

1. (AMENDED) A method for managing access to a signal representative of an event of a service provider, said method comprising:

(a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;

(b) receiving, in said smart card, data representative of a first seed value; characterized in that

(c) generating said scrambling key using said first seed value **received in said smart card** and a second seed value, said second seed value being **permanently stored** [pre-stored] in said smart card; and

(d) descrambling**, in said smart card,** said signal using said generated scrambling key to provide a descrambled signal.

5. (AMENDED) [In combination in a] **A** system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key;

(b) receiving from the service provider data representative of a first seed value, said first seed value being selected from a Euclidean plane;

characterized in that

(c) coupling said scrambled signal and said first seed value**, both received from the service provider,** to said smart card, said smart card having a means for access control processing; said access control processing means comprising means for generating said scrambling key by calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value **which is permanently stored** [, said second seed value being pre-stored] in said smart card and means for descrambling**, within said smart card,** said signal using said generated scrambling key to generate a descrambled signal; and

(d) receiving from said smart card said descrambled signal.

6. (AMENDED) The **system** [combination] of Claim 5 wherein the device is a set-top box.

7. (AMENDED) The **system** [combination] of Claim 5 wherein the device is a digital television.

REMARKS

No fee is believed to been incurred by virtue of this amendment. However, if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832.

Respectfully Submitted,
Ahmet Mursit Eskicioglu et al.

By: _____

David T. Shoneman, Attorney
Registration No. 39,371
(609) 734-9875

THOMSON multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

09/581064

ARTICLE 34

RCA 88783

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Utilizing the concept of secret sharing, the system does not require full descrambling keys to be sent to the receiving device under encryption. The keys are recovered using a seed value received from the service provider and a seed value stored in the device.

Background of the Invention

Today, a user may receive services from a variety of service providers, such as broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Most television receivers are capable of receiving unscrambled information or programs directly from broadcast and cable networks. Cable networks providing scrambled (or encrypted) programs usually require a separate stand alone set-top box to descramble (or decrypt) the program. Similarly, digital satellite systems usually provide scrambled programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card which contain the keys necessary for recovering the scrambling or descrambling keys. Protection of these important keys is paramount to prevent unauthorized copying of the programming.

European Patent Application Number EP-A-0 658 054 discloses generating a descrambling key using two pieces of transmitted data.

Summary of the Invention

In a conditional access (CA) system, the signals are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the scrambling key is

changed frequently, the period of change being as frequent as every few seconds. The protection of the descrambling keys, which need to be sent with the signals, is often provided by public-key cryptography. Public-key cryptography introduces problems associated with the public key infrastructure and distribution of the keys. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

A signal (e.g., an event or program) as described herein comprises information such as (1) audio/visual data (for example, a movie, weekly "television" show or a documentary); (2) textual data (for example, an electronic magazine, paper, or weather news); (3) computer software; (4) binary data (for example, images); (5) HTML data (for example, web pages); or any other information for which access control may be involved. The service providers include any provider broadcasting events, for example, traditional broadcast television networks, cable networks, digital satellite networks, providers of electronic list of events, such as electronic program guide providers, and in certain cases internet service providers.

Generally, the present invention defines a method for managing access to a signal, representative of an event of a service provider, utilizing a smart card. That is, this method comprises receiving in a smart card, a signal that is scrambled using a scrambling key, receiving data representative of a first seed value, generating the scrambling key using the first seed value and a second seed value that is stored in the smart card and descrambling the signal using the generated scrambling key to provide a descrambled signal.

In accordance with one aspect of the present invention, the first and second seed values are points on a Euclidean plane and the step of generating the scrambling key comprises calculating

the Y-intercept of the line formed on the Euclidean plane by the first and second seed values.

In accordance with still another aspect of the present invention, a system for managing access between a service provider and a device having a smart card coupled to the device involves the device performing the steps of receiving from the service provider a signal representative of an event that is scrambled using a scrambling key, receiving from the service provider data representative of a first seed value selected from a Euclidean plane, and coupling the scrambled signal and the first seed value to the smart card. The smart card has a means for access control processing comprising means for generating a scrambling key by calculating the Y-intercept of the line formed in the Euclidean plane by the first seed value and a second seed value stored in the smart card and means for descrambling the signal using the generated scrambling key to generate a descrambled signal.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawing

Figure 1 is a block diagram illustrating one architecture for interfacing a common set-top box to a variety of service providers.

Figure 2 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention;

Figure 3a is a graphical representation of the determination of the scrambling key in accordance with one embodiment of this invention; and

Figure 3b is a graphical representation of an allocation of a unique and non-overlapping range for each service provider in accordance with Figure 3a.

Detailed Description of the Drawing

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. The conditional access system when implemented within a device, such as a digital television, digital video cassette recorder or set-top box, provides convenient management of the descrambling keys because only a portion of the seed value necessary for key generation is stored therein. For simplicity, the below description of the invention will be directed towards an implementation using a digital television and a smart card.

In Figure 1, system 30 depicts the general architecture for managing access to a digital television (DTV) 40. Smart Card (SC) 42 is inserted into, or coupled to, a smart card reader 43 of DTV 40; an internal bus 45 interconnects DTV 40 and SC 42 thereby permitting the transfer of data therebetween. Such smart cards include ISO 7816 cards having a card body with a plurality of terminals arranged on a surface in compliance with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B. Conceptually, when such a smart card is coupled to a smart card reader, the functionality of the smart card may be considered to be a part of the functionality of the device (e.g., DTV 40) thus removing the "boundaries" created by the physical card body of the smart card.

DTV 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a cable television SP 52, a satellite system SP 54, and an internet SP 56. Conditional Access Organization (CA) 75 is not directly connected to either the service providers or STB 40 but deals with key

management and issues public and private key pairs which may be used, if necessary, as explained below.

The present invention employs the concept of secret sharing which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/visual (A/V) stream from a service provider. A variation of a secret sharing scheme, developed by Adi Shamir, is known as a threshold scheme. An (m, n) threshold scheme involves breaking a secret into n pieces (which may be called shadows), in such a way that at least m (<=n) of the pieces are required to reconstruct the secret. A perfect threshold scheme is a threshold scheme in which a knowledge of m-1 or fewer shadows provides no information about the secret. For example, with a (3,4)-threshold scheme, the secret is divided into four portions but only three of the four portions are required to reconstruct the secret. Two of the portions, however, cannot reconstruct the secret. In Shamir's (m, m) threshold scheme, choosing a higher value for m, and storing (m-1) secrets in the card would increase the system's resistance to ciphertext only attacks, but would lead to more computations for polynomial construction.

Such a threshold scheme reduces the computational requirements for the card in DES key recovery. For each new key, only a simple operation is performed (i.e., the value of the polynomial at x = 0 is computed) as compared to RSA decryption which involves modular exponentiation. Additionally, security is "perfect" (i.e., given knowledge of (x_t, y_t), all values of the secret remain equally probable).

Figures 2 and 3 together, demonstrate one embodiment of the present invention. Particularly, stored in SC 42 is a first seed value (or data point). The first seed value may be thought of as a single point on a Euclidean plane, i.e., in the form of (x0, y0). Service provider 58 transmits a signal (or event or program) that may be scrambled by a symmetric key, for example a Data Encryption Standard (DES) key. In addition to the scrambled

signal, service provider 58 transmits a second seed value. Similarly, the second seed value may be a second single point from the same Euclidean plane, i.e., in the form of (x1, y1).

The scrambled A/V signal and the second seed value is received by DTV 40 and is coupled to SC 42 for processing. SC 42 receives the second seed value and utilizes both the stored first seed value and the received second seed value to reconstruct (or recover) the symmetric key. SC 42 uses the reconstructed symmetric key to descramble the received scrambled A/V signal and generate a descrambled A/V signal. This descrambled A/V signal is provided to DTV 40 for display.

Recovery of the symmetric key is achieved by constructing a polynomial utilizing the first and the second seed values; the y-intercept of the constructed polynomial is the symmetric key. For example, given (x0, y0) and (x1, y1), the symmetric key is constructed by computing the value of $[\{(y1-y0)/(x1-x0)\}(x-x0)] + y0$ at $x = 0$. Figure 3a illustrates a graphical representation of the present invention.

Such an approach permits more than one service provider to share the stored second seed value (x0, y0). Each service provider would then be free to choose its own first seed value. The probability of constructing polynomials with identical y-intercepts (i.e., identical symmetric keys) is low. However, the range of possible second seed values could be allocated such that each service provider has a unique and non-overlapping range (see Figure 3b). Further, it is within the scope of the present invention that each service provider could choose its own first seed value which could be encrypted using the public key of the smart card before downloading. The seed value would be recovered by the smart card using its stored private key (K_{SCpri}).

The general architecture of system 30 lends itself to achieving the goal of minimizing the amount of information (or

keys) that needs to be stored in a smart card to permit access to more than one service provider.

The robustness of the defined system may be increased by scrambling portions of the event with different keys and transmitting different second seed values. Further, it is within the scope of the present invention that more than two seed values may be used to recover the symmetric key. For example, two or more seed value may be stored in the smart card and a seed value may be transmitted with the encrypted A/V signal. The symmetric key would be recovered using all of the seed values.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims.

8. The combination of Claim 5 wherein the device is a digital video cassette recorder.

Article 34

RCA 88783

Claims

1. A method for managing access to a signal representative of an event of a service provider, said method comprising:

(a) receiving said signal in a smart card, said signal being scrambled using a scrambling key;

(b) receiving, in said smart card, data representative of a first seed value;

characterized in that

(c) generating said scrambling key using said first seed value and a second seed value, said second seed value being pre-stored in said smart card; and

(d) descrambling said signal using said generated scrambling key to provide a descrambled signal.

2. The method of Claim 1 wherein said first and second seed values are points on a Euclidean plane.

3. The method of Claim 2 wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values.

4. The method of Claim 3 wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards.

ARTICLE 34

5. In combination in a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

(a) receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key;

(b) receiving from the service provider data representative of a first seed value, said first seed value being selected from a Euclidean plane; characterized in that

(c) coupling said scrambled signal and said first seed value to said smart card, said smart card having a means for access control processing; said access control processing means comprising means for generating said scrambling key by calculating the Y-intercept of a line on said Euclidean plane by said first seed value and a second seed value, said second seed value being pre-stored in said smart card and means for descrambling said signal using said generated scrambling key to generate a descrambled signal; and

(d) receiving from said smart card said descrambled signal.

6. The combination of Claim 5 wherein the device is a set-top box.

7. The combination of Claim 5 wherein the device is a digital television.

Abstract of the Disclosure

A method for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources by utilizing secret sharing for key recovery. Secret sharing eliminates the necessity to protect and transfer the complete descrambling keys between devices, because a portion of the key is stored in the device or a smart card coupled thereto.

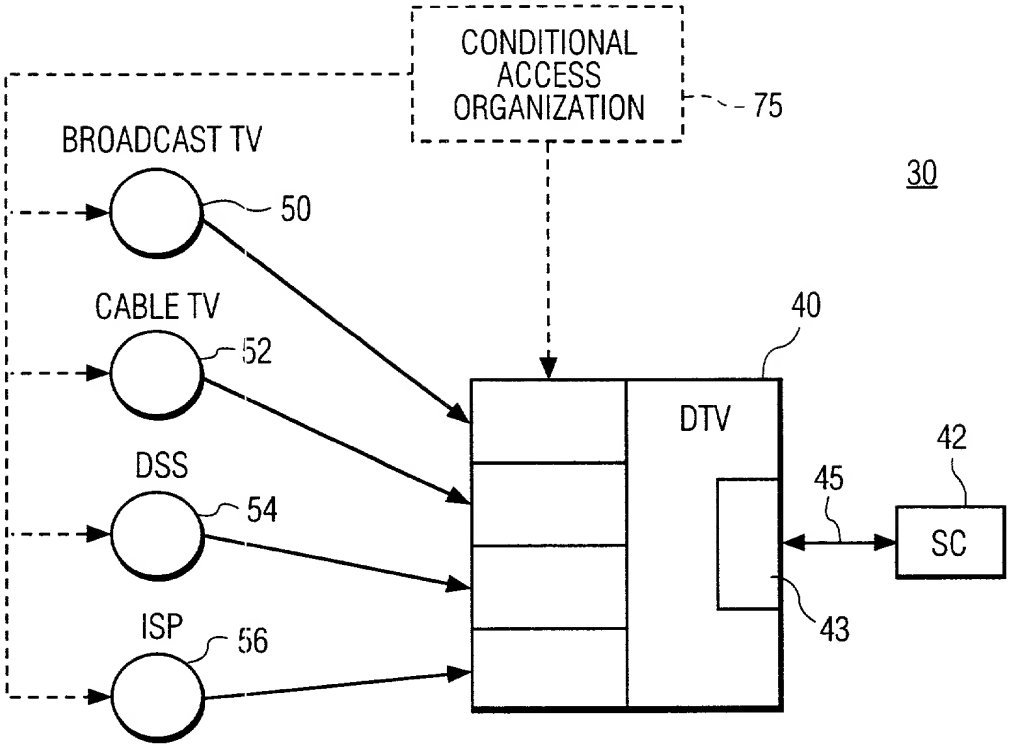


FIG. 1

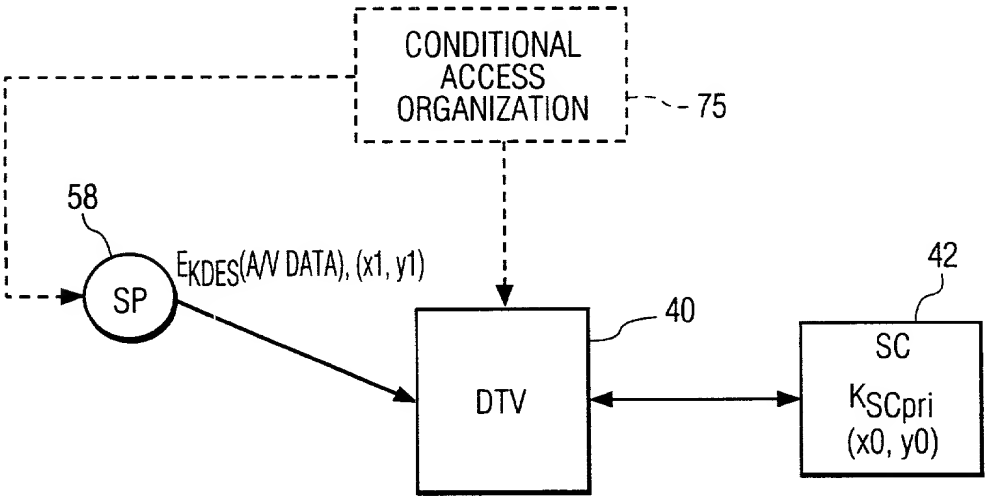


FIG. 2

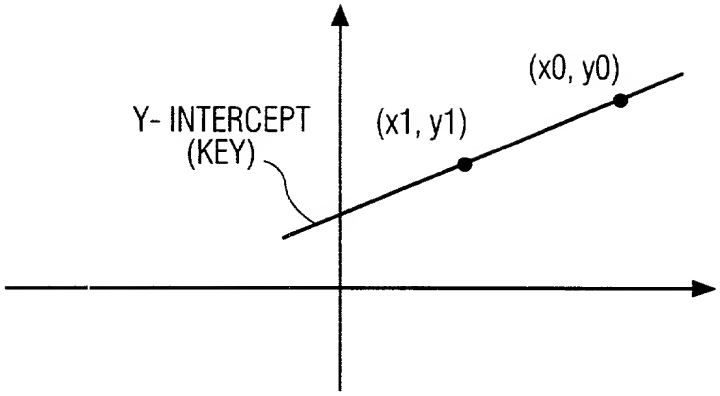


FIG. 3a

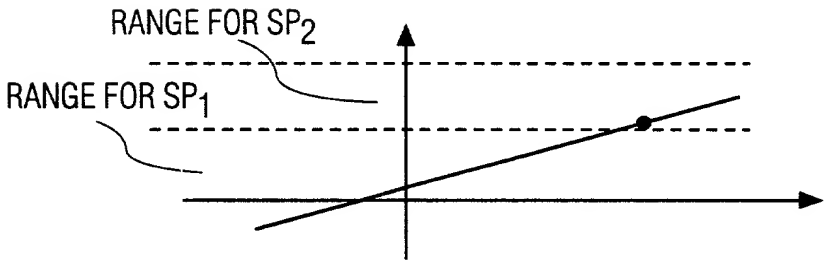


FIG. 3b

Combined Declaration For Patent Application and Power of Attorney (Continued)
(Includes Reference to PCT International Applications)

ATTORNEY'S DOCKET NUMBER: RCA 88783

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowlege the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS (Check one)		
U.S APPLICATION NUMBER	U S FILING DATE	PATENTED	PENDING	ABANDONED
60/069,063	December 10, 1997			

PCT APPLICATIONS DESIGNATING THE U.S.

PCT APPLICATION NO	PCT FILING DATE	U.S. SERIAL NUMBERS ASSIGNED (if any)			
PCT/US98/26069	09December1998(09.12.98)				

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(List name and registration number)*

Joseph S. Tripoli - Reg. No. 26,040
Joseph J. Laks - Reg. No. 27,914
David T. Shoneman - Reg. No. 39,371

Send Correspondence to:

Mr. Joseph S. Tripoli - Patent Operations
THOMSON multimedia Licensing Inc.
P.O. Box 5312
Princeton, New Jersey 08540 US

Direct Telephone Calls to: *(name and telephone number)*

1-609-734-9875

201 FULL NAME OF INVENTOR	FAMILY NAME: ESKICIOGLU	FIRST GIVEN NAME: Ahmet		SECOND GIVEN NAME: Mursit
201 RESIDENCE & CITIZENSHIP	CITY: Indianapolis	STATE OR FOREIGN COUNTRY: Indiana IN		COUNTRY OF CITIZENSHIP: TR
201 POST OFFICE ADDRESS	POST OFFICE ADDRESS: 8235 Lakeshore Trail #125	CITY: Indianapolis		STATE & ZIP CODE/COUNTRY: Indiana 46250 US
202 FULL NAME OF INVENTOR	FAMILY NAME: OZKAN	FIRST GIVEN NAME: Mehmet		SECOND GIVEN NAME: Kemal
202 RESIDENCE & CITIZENSHIP	CITY: Avcilar	STATE OR FOREIGN COUNTRY: Turkey IN		COUNTRY OF CITIZENSHIP: TR
202 POST OFFICE ADDRESS	POST OFFICE ADDRESS: Savasci Sok. Bozokatt 19/1	CITY: Avcilar		STATE & ZIP CODE/COUNTRY: Istanbul 34840, Turkey
203 FULL NAME OF INVENTOR	FAMILY NAME: BEYERS JR.	FIRST GIVEN NAME: Billy		SECOND GIVEN NAME: Wesley
203 RESIDENCE & CITIZENSHIP	CITY: Carmel	STATE OR FOREIGN COUNTRY: Indiana IN		COUNTRY OF CITIZENSHIP: US
203 POST OFFICE ADDRESS	POST OFFICE ADDRESS: 1075 Arrow Wood Drive	CITY: Carmel		STATE & ZIP CODE/COUNTRY: Indiana 46033 US

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Ahmet Mursit Eskicioglu	Mehmet Kemal Ozkan	Billy Wesley Beyers Jr.
Ahmet Mursit Eskicioglu		Billy Wesley Beyers Jr.
DATE: 10/10/2000	DATE: 2000	DATE: Oct 10 2000

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

(Includes Reference to PCT International Applications)

ATTORNEY'S DOCKET NUMBER: RCA 88783

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

the specification of which (check only one item below):

☐ is attached hereto.

☐ was filed as United States application

Serial No. _____

on _____,

and was amended

on _____ (if applicable).

☒ was filed as PCT international application

Number PCT/US98/26069

on 09 December 1998,

and was amended under PCT Article ~~19~~ 34

on December 9, 1999 (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowlege the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119
			☐ YES ☐ NO
			☐ YES ☐ NO
			☐ YES ☐ NO
			☐ YES ☐ NO
			☐ YES ☐ NO